Aula 14

DOMÍNIOS FATORIAIS

META

Estabelecer o conceito de domínio fatorial.

OBJETIVOS

Aplicar a definição de domínio fatorial na resolução de problemas.

Estabelecer a definição de máximo divisor comum em domínios fatoriais.

Reconhecer elementos primos em domínios.

PRÉ – REQUISITO

As aulas 10, 11, 12 e 13 deste curso.

INTRODUÇÃO

Quando estudamos os números inteiros, tivemos a oportunidade de verificar que os números primos (irredutíveis) do ponto de vista da divisibilidade são bastante simples, além disto, vale o teorema fundamental da Aritmética, ou seja, através da multiplicação de primos podemos gerar todos os inteiros não nulos e não invertíveis.

Nosso objetivo aqui é apresentar o conceito de domínio fatorial que é uma extensão desta propriedade dos inteiros. Ou melhor, o domínio $\mathbb{Z}$ é o primeiro exemplo de Domínio Fatorial.

O CONCEITO DE DOMÍNIO FATORIAL

Definição 1. – Dizemos que um domínio D é fatorial (ou de fatoração única) se as seguintes condições são satisfeitas:

i) Todo elemento a não nulo e não invertível admite uma fatoração do tipo:
$a = u.p_1. \ldots .p_r$ $(\star)$
Onde $u \in \cup(D)$ e $p_1, \ldots, p_r \in D$ são irredutíveis.

ii) Se um elemento $a\,(a \notin \cup(D) \cup \{0\})$ admite duas fatorações $a = u.p_1. \ldots .p_r$ e $a = u'.p'_1. \ldots .p'_s$ do tipo $(\star)$ então $r = s$ e existe uma permutação $\sigma \in S_r$ tal que $p_i = p'_{\sigma(i)}$ para $i = 1, 2, \ldots, r$.

Informalmente, num Domínio Fatorial (DFU) todo elemento não nulo e não invertível ou é irredutível ou é um produto de elementos irredutíveis, e esta fatoração é única, a menor da ordem dos fatores e de multiplicação por invertíveis.

Exemplo 1. Segue do teorema Fundamental da Aritmética que $\mathbb{Z}$ é um DFU.

A proposição a seguir fornece uma caracterização dos domínios fatoriais da qual podemos concluir que todo domínio principal (e, portanto todo domínio euclidiano) é fatorial.

Proposição 1. Seja D um domínio. Então D é um Domínio Fatorial se, e somente se valem as seguintes proposições:

i) Todo elemento irredutível de D é primo.
ii) Toda cadeia ascendente de ideais principais de D é estacionária, isto é, se $(d_1) \subset (d_2) \subset \ldots \subset (d_n) \subset \ldots$ é uma sequência de ideais, então existe um $m \in \{1, 2, \ldots\}$ tal que, $\forall n \geq m, d_n = d_m$.

Demonstração. $(\Longrightarrow)$ Sejam $p, a, b \in D$ onde p é irredutível e $p|ab$. Então existe $c \in D$ tal que $pc = ab$. Como $a, b, c \notin \cup(D) \cup \{0\}$, e D é fatorial, a, b e c possuem fatorações do tipo $(\star)$, ou seja,

$a = u.p_1. \ldots .p_r$
$b = u'.p'_1. \ldots .p'_s$

$$c = u''.p''_1. \dots .p''_t$$

Pela unicidade da fatoração de pc (ou ab) segue que p é associado de um p_i ou de um q_j. No primeiro caso, $p|a$ e no segundo $p|b$. Portanto p é primo.

Por outro lado, consideremos uma cadeia ascendente de ideais principais

$$(d_1) \subset (d_2) \subset \dots \subset (d_n) \subset \dots .$$

Como $d_i|d_1$ para $i \in \{1, 2, \dots\}$, as fatorações de d_1 e d_i têm as formas

$$d_1 = u.p_1. \dots .p_r$$
$$d_i = u'.p_1. \dots .p_s$$

Onde $r \leq s$. Logo para algum $m \in \{1, 2, \dots\}$ temos que d_m é associado de $d_n, \forall n \geq m$ e consequentemente

$$(d_m) = (d_{m+1}) = \cdots$$

Ou seja, a cadeia $(d_1) \subset (d_2) \subset \cdots$ é estacionária.

($\Longleftarrow$) Agora, suponhamos que *D* é um domínio para o qual valem "i)" e "ii)". Seja $a \in D$ um elemento não nulo e não invertível, e suponhamos, por contradição, que *a* não tenha uma fatoração do tipo ($\star$).

Então, $a = bc$ onde a ou *b* não admite uma fatoração do tipo ($\star$) e ambos são não nulos e não invertíveis. Fazendo $a_1 = a$ e escolhendo a_2 um elemento entre *b* e *c* que não admite uma fatoração do tipo ($\star$), por indução construímos uma sequência

$(a_1, a_2, \dots, a_n, \dots)$ onde, $a_{i+1}|a_i$ e $a_{i+1} \nsim a_i$.

Segue que os ideais principais (a_n) são tais que

$$(a_1) \subsetneq (a_2) \subsetneq \dots \subsetneq (a_n) \subsetneq \dots$$

Contrariando a hipótese de que toda cadeia ascendente é estacionária. Portanto, o domínio *D* é fatorial.

Observação. Sabemos que todo domínio euclidiano é de ideais principais e que em todo domínio de ideais principais, ser irredutível implica ser primo e toda cadeia ascendente de ideais estabiliza. Do teorema acima segue que todo domínio principal é fatorial.

Exemplo 2. Considerando a observação acima podemos afirmar que $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$ são domínios fatoriais.

Observação. Lembremos que um corpo é um domínio euclidiano no qual não existem irredutíveis. Neste caso extremo, temos um Domínio Fatorial onde os tais elementos não nulos e não invertíveis se existissem seriam produtos de irredutíveis.

Observação. No curso de Estruturas Algébricas II, você caro aluno, estudará anéis de polinômios numa indeterminada sobre domínios. Em particular, o anel dos polinômios em uma indeterminada com coeficientes inteiros é um exemplo de domínio fatorial que não é principal.

Vamos terminar esta aula estudando o exemplo de Kummer de um domínio que não é fatorial. Trata-se do conjunto $D = \mathbb{Z}[\sqrt{5}i] = \{\alpha = a + b\sqrt{5}i\, ; a, b \in \mathbb{Z}\}$.

É fácil verificar que *D* é um subdomínio do corpo dos números complexos.

A função norma $N: \mathbb{Z}[\sqrt{5}i] \to \mathbb{N}$ dada por $\mathbb{N}(\alpha) = |\alpha|^2$ que inclusive já estudamos as respectivas de $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$ tem aqui também um papel importante.

Proposição 2. Seja $\alpha \in \mathbb{Z}[\sqrt{5}i]$. As afirmações a seguir são equivalentes:

i) $\alpha \in \cup\left(\mathbb{Z}[\sqrt{5}i]\right)$;
ii) $N(\alpha) = 1$;
iii) $\cup\left(\mathbb{Z}[\sqrt{5}i]\right) = \{-1, 1\}$

Demonstração. (Atividade)

Proposição 3. Seja $\alpha = a + b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ não nulo e não invertível. Se, para cada divisor *d* de $a^2 + 5b^2, d \neq a^2 + 5d^2$, a equação diofantina $x^2 + 5y^2 = d$ Não tem solução, então α é um elemento irredutível.

Demonstração. Suponhamos, por contradição, que α seja irredutível e seja $\alpha = (c + d\sqrt{5}i).(e + f\sqrt{5}i)$. Onde os fatores $c + d\sqrt{5}i$ e $e + f\sqrt{5}i$ são não nulos e não invertíveis em $\mathbb{Z}_{[\sqrt{5}i]}$. Da proposição anterior, $N(c + d\sqrt{5}i) \neq 1$ e $N(e + f\sqrt{5}i) \neq 1$. Logo, $N(\alpha) = a^2 + 5b^2 = (c^2 + 5d^2).(e^2 + 5f^2)$.

Assim, para $d = e^2 + 5f^2 \neq a^2 + 5b^2$, o par (c, d) é uma solução da equação diofantina $x^2 + 5y^2 = d$, uma contradição.

Exemplo 14.2.3. É fácil ver que para $d \in \{1,2\}$, divisor próprio de $2^2 + 5.0^2$, a equação diofantina $x^2 + 5y^2 = d$ não tem solução. Portanto, $\alpha = 2 = 2 + 0.\sqrt{5}i$ é irredutível em $\mathbb{Z}[\sqrt{5}i]$.

Analogamente, para $d \in \{1,3\}$, a equação diofantina também não tem solução. Portanto 3 também é irredutível em $\mathbb{Z}[\sqrt{5}i]$.

Exemplo 14.2.4. Os elementos $1 - \sqrt{5}i$ e $1 + \sqrt{5}i$ são irredutíveis em $\mathbb{Z}[i]$, pois para cada divisor próprio de $1^2 + 5.(\pm 1)^2$ que pertence ao conjunto $\{1,2,3\}$, a equação diofantina $x^2 + 5y^2 = d$ não admite solução.

Agora considerando os conteúdos dos exemplos *14.2.3* e *14.2.4* e notando que $2.3 = (1 - \sqrt{5}i).(1 + \sqrt{5}i) = 6$ temos que, em $\mathbb{Z}[i]$, o elemento 6 admite duas fatorações distintas como produto de irredutíveis, donde concluímos que $\mathbb{Z}[i]$ é um domínio que não é fatorial. No-

temos ainda que, por exemplo, 2 não é primo em $\mathbb{Z}[i]$, haja visto que $2|(1-\sqrt{5}i).(1+\sqrt{5}i)$, $2 \nmid (1-\sqrt{5}i)$ e $2 \nmid (1+\sqrt{5}i)$.

RESUMO

Nesta aula, caro aluno, definimos Domínios Fatoriais, estabelecemos uma primeira caracterização dos Domínios Fatoriais, da qual concluímos que domínios principais são fatoriais e terminamos a aula estabelecendo o exemplo de Kummer de um Domínio que não é fatorial.

ATIVIDADES

1. Seja *a* um inteiro positivo e seja $\alpha \in \mathbb{R}$ tal que $10^{\alpha} = a$ (ou seja, $\alpha = \log_{10} a$). Prove que α não é racional.
2. Sejam $a = {p_1}^{m_1}. \dots .{p_r}^{m_r}$ e $b = {p_1}^{n_1}. \dots .{p_r}^{n_r}$ as fatorações em primos positivos dos inteiros *a* e *b* onde, $m_i, n_i \in \mathbb{N}$. Prove que $mdc(a,b) = {p_1}^{k_1}. \dots .{p_r}^{k_r}$ e $mmc(a,b) = {p_1}^{l_1}. \dots .{p_r}^{l_r}$ onde $l_i = mín\{m_i, n_i\}$ e $k_i = máx\{m_i, n_i\}$ para $i = 0,1, \dots, r$.
3. Prove que os elementos a e b da atividade 2, verificam a relação: $mdc(a,b).mmc(a,b) = ab$.
4. Num Domínio Fatorial, um elemento d é um máximo divisor comum dos elementos não nulos a e b se, $d|a,b$ e se existe $d' \in D$ tal que $d'|a,b$ então $d'|d$. Se $a,b \notin \cup(D) \cup \{0\}$, escreva d em função dos fatores irredutíveis de a e b.
5. Mostre que se α é um elemento primo do domínio de Kummer então α divide um elemento primo de $\mathbb{Z}$.

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade, caro aluno, você deve ter assumido, por contradição, que α é racional contrariando o fato de que $\mathbb{Z}$ é um Domínio Fatorial.

Nas segunda e terceira atividades você, usando as respectivas definições de mdc e mmc não deve ter tido dificuldades para provar tais afirmações.

Na quarta atividade, você deve ter usado o caso especial da atividade 2 como inspiração.

Na quinta atividade, se você caro aluno, conseguiu êxito, deve ter notado que $N(\alpha) \in \{2,3,4,6, \dots\}$ e usado o teorema fundamental da Aritmética.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).